20 is rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes in view of "Distributed Provers with Applications to Undeniable Signatures" by Pedersen. Finally, claim 21 is rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes in view of Pedersen, in further view of Computer Architecture: A Quantitative Approach, Second Edition by Patterson and Hennessey.

Claims 23 and 24 are allowed. Claims 2-10 and 12-21 are objected to as being dependent upon a rejected base claim.

Applicant traverses the objection to the drawings under 37 C.F.R. §1.83(a). In addition, Applicant traverses the §102(b) and §103(a) rejections. Applicant respectfully requests reconsideration of the present application in view of the following remarks.

Applicant initially notes that the Examiner rejects claims 2, 6, 12 and 16 under §102(b) and claims 3, 13, 20 and 21 under §103(a), but then states on page 6 of the Office Action:

> Claims 2-10 & 12-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicant respectfully submits that these inconsistencies make the rejections to claims 2, 3, 6, 12, 13, 16, 20 and 21 improper. Nonetheless, the Applicant will proceed to address the §102(b) and §103(a) rejections of these claims in these remarks.

In formulating his 37 C.F.R. §1.83(a) objection to the drawings, the Examiner states:

> The drawings must show every feature of the invention specified in the claims. Therefore, the process steps of claims 8, 18, 23 and 24 (key transformation) must be shown or the feature(s) canceled from the claim(s). (Office Action, page 2, section 3).

Applicant respectfully submits that the features of claims 8, 18, 23 and 24 are, in fact, present in the drawings as originally filed. For efficiency and ease of understanding, Applicant shows some general features of the present invention in the figures in the form of illustrative embodiments. By way of example, the specification at page 5, line 28, to page 6, line 4 indicates that process steps

such as those recited may be implemented in software stored in memories 22A, 22B of FIG. 1. Also, the specification at page 6, line 16, to page 7, line 6, and page 8, line 1 to page 9, line 6, indicates that the process steps at issue are in fact shown in generalized form in the flow diagram of FIG. 2. Therefore, it is believed that the features of claims 8, 18, 23 and 24 are aptly shown in the drawings through the use of illustrative embodiments.

With regard to the §102(b) rejection of claims 1, 2, 6, 11, 12, 16, 22, 25, 26 and 27, Applicant notes that the Manual of Patent Examination, Eighth Edition, August 2001 (MPEP) §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Each of independent claims 1, 11, 22, 25, 26 and 27 includes an element comprising information representative of first and second proofs, "wherein the first proof is a proof that the operation has been correctly performed, and the second proof is a proof that the first proof has been correctly performed." In formulating his §102(b) rejection, the Examiner states that Menezes, page 477, steps 1-7 teaches a first proof "that the operation . . . has been correctly performed," and step 8 teaches a second proof "that the first proof was correctly performed." Applicant respectfully disagrees. Menezes describes a situation wherein entity *A* digitally signs a message and entity *B* attempts to verify this digital signature (Menezes, page 476, §11.122). In step 8:

> *B* computes [*c*] and [*c* ']. If $c = c'$, then *B* concludes that *s* is a forgery; otherwise *B* concludes that the signature is valid and *A* is attempting to disavow the signature *s*.

As Menezes states explicitly on page 477, this step "verif[ies] that *A* has performed the protocol correctly." (Menezes, page 477, description of Protocol 11.125, emphasis added.) Step 8, therefore, relates to the correct performance of an operation by *A*; step 8 does not signal the correct performance of a proof, which would, if steps 1-7 were assumed to be such a proof, entail that step

8 signal the correctness of operations by entity *B*. Therefore, step 8 fails teach a second proof that the first proof has been correctly performed. Correspondingly, the Menezes reference fails to teach each and every element contained in claims 1, 11, 22, 25, 26, and 27.

Furthermore, claims 1, 11 and 22 also each contain steps comprising "transmitting the proof information signal from the prover to the verifier." The Examiner in formulating his §102(b) rejections states that Menezes, page 477, steps 3 and 6 anticipate this element. The Applicant respectfully disagrees. Menezes in steps 3 and 6 teaches that "*A* computes [*w* or *w'*] and sends [*w* or *w'*] to *B*," where *w* and *w'* are variables exchanged as part of the signature verification process. In comparison, the "proof information" transmitted in claims 1, 11 and 22 is "at least one signal corresponding to information representative of first and second proofs." Therefore, the transmitted information in the Menezes reference and the claims at issue are different types of information. For this reason, the Menezes reference fails to teach each and every element contained in claims 1, 11 and 22.

Therefore, since each of independent claims 1, 11, 22, 25, 26 and 27 includes at least one element not disclosed in Menezes, these claims are not anticipated by Menezes. Dependent claims 2, 6, 12 and 16 are believed allowable for at least the reasons identified above with regard to their respective independent claims.

With respect to the §103(a) rejections, Applicant initially notes that MPEP §2143.03 states that in order "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art," citing In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Applicants also note that MPEP §2143.03 provides that "[i]f an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious," citing In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

In forming his §103(a) rejection of dependent claims 3, 13, 20 and 21, the Examiner fails to provide any additional argumentation that the particular dependent claim limitations are obvious in view of the proposed combinations of references. Therefore, Applicant respectfully submits that the Examiner has failed to support a conclusion of *prima facie* obviousness for the dependent claims at least for the reason that the proposed combinations fail to supplement the above-described deficiencies of Menezes as applied to independent claims 1 and 11. Thus the proposed combinations

fail to teach or suggest all the claim limitations in independent claims 1 and 11, as discussed above with regard to the §102(b) rejections.

It is further noted, in formulating his §103(a) objection to claims 3, 13, 20 and 21, the Examiner variously states:

> One of ordinary skill in the art would have been motivated to perform such a modification to prevent the signer from observing the message it signs.
>
> . . .
>
> One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without having to give away a secret.
>
> . . .
>
> One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without the signer having to give away the secret.
>
> . . .
>
> One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of increased performance and improved availability.
>
> (Office Action, pages 4 -5).

The Federal Circuit has stated that when patentability turns on the questions of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual questions of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344. Applicants respectfully submit that there has been no such showing in the present §103(a) rejections of such objective evidence of record that would motivate one skilled in the art to modify or combine the proposed references and reference combinations. Instead the above quoted language is precisely the type of subjective, conclusory statements that the Federal Circuit has indicated provides insufficient support for an obviousness rejection.

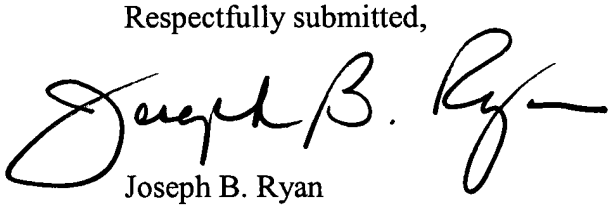
Finally regarding the accepted claims, Applicant would like to clarify a statement made by the Examiner with respect to prior art. With respect to claims 8, 18, 23 and 24, the Examiner states that "the prior art teaches, as stated by the applicant of the present invention (page 1 of specification), taking an input of (g, y, m, s) for which $\log_g y = \log_m s$." (Office Action, page 6). The above-referenced portion of the specification in fact states:

> An example of a protocol which may leak information when given invalid inputs is based on the techniques described in D. Chaum and H. Van Antwerpen, "Undeniable Signatures," Advances in Cryptology-Proceedings of Crypto '89, pp. 212-216, which attempt to determine whether a given quadruple (g, y, m, s) satisfies the relation $\log_g y = \log_m s$ in the context of verifying the validity of undeniable signatures.

To the extent the characterization of the prior art as proffered by the Examiner differs from the actual language of the specification, the characterization is respectfully traversed.

In view of the above, Applicant believes that claims 1-22 and 25-27 are in condition for allowance. Applicant respectfully requests the withdrawal of the 37 C.F.R. §1.83(a) objection with respect to the drawings, and the §102(b) and §103(a) rejections with respect to the claims.

Respectfully submitted,



Date: April 13, 2004

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517